RESPONSE

Claims Status

Claims 1-8 were originally filed in this application. In an Office Action dated December 16, 2004, Claims 1-8 were rejected, and an amendment and response was filed on May 9, 2005 in response thereto. A final Office Action was mailed on August 5, 2005, maintaining the rejection of claims 1-8. A subsequent Amendment and Response was filed on December 5, 2005, as part of a Request for Continued Examination in which Applicant amended the specification, cancelled claims 1 and 6-8, amended claims 2-5, and added new claims 9-16. In an Office Action dated March 6, 2006, claims 2-5 and 9-16 were rejected. A subsequent Amendment and Response was filed on May 25, 2005, in which Applicant amended claims 4, 5, 9, 11, 13, 15 and 16. A final Office Action was mailed on July 31, 2006, in which new grounds for rejection were cited.

Applicant submits this paper to address these new rejections and to more particularly point out and distinctly claim the subject matter which Applicant regards as the invention. No new matter has been added.

Claim Objections

Claims 2, 5 and 21 have been objected to for certain non-substantive issues. Applicant has amended claims 2 and 5 and cancelled claim 12 to address these objections.

Claim Rejections

Claims 3-5 and 9 and 11-16 have been rejected under 35 U.S.C. 103(a) over U.S. Patent No. 5,420,866 to Wasilewski ("Wasilewski") in view of U.S. Patent No. 6,735,313 to Bleichenbacher et al. ("Bleichenbacher"), U.S. Patent No. 6,212,633 to Levy et al. ("Levy"), and U.S. Patent No. 5,963,909 to Warren et al. ("Warren").

Claim 2 has been rejected under 35 U.S.C. 103(a) over Wasilewski in view of Bleichenbacher, Levy, and Warrant and in further view of U.S. Patent No. 5,768,381 to Hawthorne ("Hawthorne").

Independent Claims 9 and 13

Independent claims 9 and 13, as amended, each recite using unique packet *keys* based on a base key and unique packet *tags* to encrypt or decrypt secure content at transmission (claim 9) or receipt (claim 13), and transmitting the encrypted base key and encrypted packets in separate transmissions. More specifically, claim 9 recites, in part, encrypting each data packet of a media stream using unique packet keys based on a base key, which is then encrypted. The encrypted base key (i.e., the open key) is transmitted to the recipient, and the encrypted data packets are sent "in a transmission separate from the transmission of the open key." Likewise, claim 13 recites, in part, "receiving, in a first transmission, an encrypted packet stream" and "in a second transmission an encrypted base key." As a result, the key used for encrypting and decrypting the encrypted packet stream is sent separately from the media stream for which the key was used. See, for example, paragraph 0031 of the application as published.

None of the cited references contemplates using packet-specific tags and a base key that are sent separately from the encoded data. In each case, and in contrast to the claims as amended, the key used to encrypt (or decrypt) transmitted content is sent with the content itself. Specifically, Bleichenbacher describes a system "which transmits a program identifier with the encrypted programming content." Abstract. Similarly, the Wasilewski system provides "different sets of conditional access information to a remote location" by, in part "inserting the set of conditional access information into a respective sequence of transport packets." (Abstract.) Wasilewski goes further, stating that "the Entitlement Control Messages for each elementary stream are inserted into respective transport packets." (Col. 9, lines 60-62.) Warren also describes a system in which "source material is scrambled (e.g., encrypted) according to an encryption key, and the encryption key is embedded in the data layer." (Col. 14, lines 4-6.)

This distinction confers important advantages. Because Applicant's invention uses encrypted packet keys that are based on a unique packet tag and a base key that is not transmitted with the encrypted media, no one data stream contains all of the necessary components for decrypting the packets. By sending the key separately from the media, the invention overcomes a significant security shortcoming of previous approaches, namely, the contemporaneous transmission of encrypted data and key used to decrypt the data.

Thus, Applicant respectfully submits that independent claims 9 and 13, as well as those claims that depend therefrom, are patentable over the cited references.
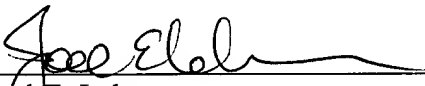
CONCLUSION

Applicant respectfully requests reconsideration of the application and claims in light of this Response, and respectfully submits that the claims are in condition for allowance. If the Examiner believes, in his review of this Response or after further examination, a telephonic interview would expedite the favorable prosecution of the present application, the Applicant's attorney would welcome the opportunity to discuss any outstanding issues, and to work with the Examiner toward placing the application in condition for allowance.

Respectfully submitted,

Date: October 11, 2006
Reg. No. 56,401

Joel E. Lehrer
Attorney for Applicants
Goodwin Procter LLP
Exchange Place

Tel. No.: (617) 570-1057
Fax No.: (617) 523-1231

Boston, Massachusetts 02109
Customer No. 051414